UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-80

21-093-04

REDACTED SEARCH AND SEIZURE WARRANT

TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An application by a federal law enforcement officer or an attorney for the government requests the search of the following property more fully described in Attachment A, attached hereto and incorporated herein by reference.

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the property described above, and that such search will reveal evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography), which is more fully described in Attachment B, attached hereto and incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before June 24, 2021 (not to exceed 14 days)
☑ in the daytime – 6:00 a.m. to 10:00 p.m.
☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the undersigned Judge.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized,
☐ for _____ days *(not to exceed 30).*

☐ until, the facts justifying, the later specific date of _____.

June 10, 2021 @ 5:12 p.m. central time at Pierre, South Dakota

Date and Time Issued via video

Mark A. Moreno

MARK A. MORENO
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-80

21-093-04 **REDACTED RETURN**

Date and time warrant executed: _____

Copy of warrant and inventory left with: _____

Inventory made in the presence of: _____

Inventory of the property taken and name of any person(s) seized (attach additional sheets, if necessary):

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

David Hohn, Special Agent
Homeland Security Investigations

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No.: 4:21-mj-80

21-093-04 **REDACTED ATTACHMENT A**

Location to be searched

The property to be searched is the MediaLab KIK account with a username of "[redacted]" and a display name of "[redacted]" that is stored at premises owned, maintained, controlled, or operated by KIK Interactive, headquartered at 1237 7th Street Santa Monica, CA 90401 hereinafter referred to as "premises," and further described in Attachment A hereto.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No.: 4:21-mj-80

21-093-04 **REDACTED ATTACHMENT B**

Items to be seized

I. Information to be disclosed by KIK, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab (KIK), including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab (KIK), or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), KIK is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the KIK accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and emails "invites" sent or received via KIK, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books,

contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between KIK and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A involving the account associated the KIK account with a username of "[redacted]" and a display name of "[redacted]" pertaining to the possession and distribution of child pornography images.

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to the Special Agent designated on the fax cover sheet located at the address 2708 North 1st Ave Sioux Falls, SD 57104.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding:

21-093-04

No. 4:21-mj-80

REDACTED APPLICATION FOR SEARCH AND SEIZURE WARRANT

I, David Hohn, being duly sworn depose and say:

I am a Special Agent with the Homeland Security Investigations, and have reason to believe that on the property or premises as fully described in Attachment A, attached hereto and incorporated herein by reference, there is now concealed certain property, namely: that which is fully described in Attachment B, attached hereto and incorporated herein by reference, which I believe is property constituting evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, concerning violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography).

The facts to support a finding of Probable Cause are contained in my Affidavit filed herewith.

David Hohn, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me, via video, on the 10th day of June, 2021, at Pierre, South Dakota.

MARK A. MORENO
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding:	No.: 4:21-mj-80
21-093-04	**REDACTED AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION**

STATE OF SOUTH DAKOTA)
) SS
COUNTY OF MINNEHAHA)

I, David Hohn, being first duly sworn on oath, deposes and states:

1. I am a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) in Sioux Falls, South Dakota and have been duly employed in this position since January 2020. I am a graduate of the Criminal Investigator Training Program and ICE Special Agent Training Program at the Federal Law Enforcement Training Center. Prior to my employment with HSI, I was a United States Probation officer for eleven years. I have received specialized training pertaining to conducting criminal investigations, immigration and customs laws, investigative techniques, searching databases, conducting interviews, executing search warrants, and making arrests with respect to criminal violations of United States Code.

2. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of United States Statues 18 U.S.C. §§ 2251, 2252, and 2252A,

involving violations of law involving child pornography and 18 U.S.C. § 2422(b), enticement of a minor using the internet. During my law enforcement career, I have become familiar with the modus operandi of persons involved in the illegal production, distribution and possession of child pornography and those who engage in enticement of minors using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. I have been informed that 18 U.S.C. § 2422(b) prohibits enticing minors to engage in sexual acts and that 18 U.S.C. §§ 2251, 2252, and 2252A prohibit the manufacture, distribution, receipt, and possession of child pornography. Additionally, I have been informed that 18 U.S.C. § 1466A prohibits the distribution of visual representations of the sexual abuse of children and that such depictions include cartoon images.

4. The facts set forth in this affidavit are based on my personal knowledge; knowledge obtained from other individuals, including other law enforcement officers; interviews of persons with knowledge; my review of documents, interview reports and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, no

information known to me that would tend to negate probable cause has been withheld from this affidavit.

5. I make this affidavit in support of an application for a search warrant for information associated with the KIK account with a username of "[redacted]" and a display name of "[redacted]" that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc. (KIK), headquartered at 1222 6th Street Santa Monica, CA 90401 hereinafter referred to as "premises," and further described in Attachment A hereto.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this affidavit and Attachments A and B:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of

themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output

devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

j. "Electronic Storage Device" includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

l. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

m. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

n. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

p. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the

Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

r. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD EXPLOITATION AND CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

8. I have had both training and experience in the investigation of computer related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve many functions for persons who exploit children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.

b. Persons who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the

photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography and other materials used for the online child exploitation. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera

or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.

f. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

KIK Background

9. Kik advertises itself as "the first smartphone messenger with a built-in browser." Kik Messenger allows its users to "talk to your friends and browse and share any web site with your friends on Kik." Kik believes it is at

the forefront of the "new era of the mobile web." Kik was founded in 2009 by a group of University of Waterloo students who started a company designed to "shift the center of computing from the PC to the phone." According to the website, Kik Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control of with whom they communicate. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even more with mobile web pages.

10. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads and is available on the Google PlayStore for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

11. In general, providers like Kik ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address. However, the accuracy of this information is not verified by Kik.

12. Kik typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized,

the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. Kik often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. In addition, generally Kik maintains at least the last 30 days of all communications for each Kik user and will produce these records when requested pursuant to a search warrant.

13. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

14. In October 2019, Kik was purchased by MediaLab, a company operating in the United States. Given the ability for users to create multiple accounts that are not linked to a specific mobile device (i.e. a phone number), it has become a popular app used by people involved in the collection, receipt, and distribution of child pornography.

DROPBOX INC.

15. "Dropbox" refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

16. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

17. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

18. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

19. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers

typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND OF THE INVESTIGATION

20. On April 13, 2021, I received a cyber tip from the South Dakota Internet Crimes Against Children (ICAC) Task Force. The cyber tip came from the National Center for Missing and Exploited Children (NCMEC) regarding a Dropbox account with the username "[redacted]" and email address [redacted]. The cyber tip included IP addresses which had accessed the Dropbox account.

21. An IP address which accessed the Dropbox account on [redacted] was identified as [redacted]. A reverse IP address lookup found this IP address is registered to Midcontinent Communications with a possible subscriber location in Sioux Falls, South Dakota. A summons was sent to Midco Communications requesting subscriber information for the IP address. Midco Communications responded stating on [redacted], this IP address was leased to [redacted] located at [redacted], Sioux Falls, SD 57104-1947.

22. Accurint showed the email account [redacted] belongs to a [redacted] with a residential address of [redacted], Canton SD 57103-1653. A subpoena to Gmail showed the subscriber for the email account [redacted] signed up for the

account using the name [redacted] with a residence in Sioux Falls, South Dakota.

23. The cyber tip also included two video files depicting suspected child pornography. I reviewed the video files which are described below:

Filename: Video [redacted]
Description: [redacted].

Filename: Video [redacted]
Description: [redacted].

24. On May 6, 2021, Magistrate Judge Veronica L. Duffy in the District of South Dakota signed a search warrant for the Dropbox account with the username "[redacted]" and email address [redacted]. On May 17, 2021, I viewed the results of the Dropbox search warrant which were received on May 6, 2021. A review of the file date showed all the video files in the account were added on [redacted].

25. The Dropbox account contained three folders intitled: "[redacted]", "[redacted]", and "[redacted]". The "[redacted]" folder contained

18 videos of age difficult pornography. The "[redacted]" personal folder contained 38 pictures and 8 videos of adult or age difficult pornography. In the folder entitled "[redacted]" there were 118 videos. At least 22 of the videos in the folder appeared to be child pornography videos and the rest of the videos were age difficult or adult pornography. I viewed the videos; a description of 3 of the child pornography videos is provided.

Filename: Video [redacted]
Description: [redacted]

Filename: [redacted]
Description: [redacted]

[redacted]

Filename: [redacted]
Description: [redacted]

26. On June 2, 2021, U.S. Magistrate Judge Mark A. Moreno signed a search warrant for [redacted] in Watertown, SD.

27. During the search, [redacted]

[redacted].

28. After downloading the files, [redacted].

29. This investigation revealed that [redacted].

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND/OR WHO RECEIVE AND/OR POSSESS CHILD PORNOGRAPHY

30. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law

enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years

and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

CONCLUSION

31. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit this Affidavit in support of probable cause for a Warrant to search the location described in Attachment A. The facts outlined above show that the account listed in Attachment A have been used for the exploitation of children using the internet including violations of 18 U.S.C. §§ 2251, 2252, 2252A (production, receipt and possession of child pornography), which items are more specifically described in Attachment B.

David Hohn
Special Agent
Homeland Security Investigation

Subscribed and sworn to before me, via video, on the 10th day of June 2021, at Pierre, South Dakota.

MARK A. MORENO
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No.: 4:21-mj-80

21-093-04 **REDACTED ATTACHMENT A**

Location to be searched

The property to be searched is the MediaLab KIK account with a username of "[redacted]" and a display name of "[redacted]" that is stored at premises owned, maintained, controlled, or operated by KIK Interactive, headquartered at 1237 7th Street Santa Monica, CA 90401 hereinafter referred to as "premises," and further described in Attachment A hereto.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No.: 4:21-mj-80

21-093-04

REDACTED ATTACHMENT B

Items to be seized

I. Information to be disclosed by KIK, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab (KIK), including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab (KIK), or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), KIK is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the KIK accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and emails "invites" sent or received via KIK, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books,

contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between KIK and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A involving the account associated the KIK account with a username of "[redacted]" and a display name of "[redacted]" pertaining to the possession and distribution of child pornography images.

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to the Special Agent designated on the fax cover sheet located at the address 2708 North 1st Ave Sioux Falls, SD 57104.